Worksheet Instructions for:
Evaluating Controls over Automated Information Systems
"Application Specific Controls"

General Instructions and Considerations

Due to the formation of the Department of Information Technology (DIT), many IT related responsibilities that were formerly assumed by agency/department Management has shifted to Department of Information Technology (DIT) management. DIT management is responsible for the State of Michigan's General Controls environment, while agency management are the business process/application owners and, therefore, hold responsibility for managing their Application Specific Controls and their Application Environment Controls. As part of the ongoing evaluation of internal controls and the biennial internal control evaluation reporting process, DIT management developed a "General Controls" worksheet to document controls over the Statewide general IT environment. In addition, worksheets exist for business process owners to evaluate "Application Specific" and "Application Environment" controls. These evaluation tools are essential for departments responsible for administering critical information systems that support departmental business processes.

CobiT (Control Objectives for Information and Related Technology), developed by the Information Systems Audit and Control Foundation (ISACF), was used as a foundation in preparing the General Controls, Application Specific Controls and Application Environment Controls worksheets. CobiT is designed for use by IT management/users and information systems auditors, and is considered one of the most effective and widely accepted tools for evaluating security and control in the IT environment.

"General Controls" (instructions (doc) (pdf), worksheets (doc) (pdf)) relate to activities that provide for the proper operation of application systems. General controls encompass strategic planning, business continuity, contingency planning, system development methodology, procedures for documenting, reviewing, testing, and approving system changes, and a variety of other control activities.

"Application Environment" controls (instructions (doc) (pdf), worksheets (doc) (pdf)) relate to the environment in which the agency's various computer applications reside. Controls are focused toward service level agreements, data storage and back up, end user support, and others. If controls over the application environment are the same across all agency applications, the worksheet will only need to be completed once.

"Application Specific" controls focus on input, processing, and output controls over the application. These controls should be evaluated for each application that the agency deems critical to accomplish their business objectives. More specific instructions for utilizing the Application Specific Controls worksheets (doc) (pdf) are provided below.

Collaboration between IT personnel and non-IT activity managers is necessary to evaluate risks/controls over the objectives listed on the worksheet(s).

It is critical to document the agency's internal control structure/systems, in addition to evaluating the control structure. In past biennial evaluations, documentation efforts have not been sufficiently addressed, particularly for each department's unique IT environment. Improved documentation will reduce efforts/resources required to complete the next biennial evaluation and facilitate periodic monitoring of controls by managers of the information systems.

(You may customize the worksheet during the evaluation process to meet your specific needs or if using it for the first time, but the standard worksheet is recommended.)

Specific Instructions

There is one worksheet to be used when evaluating application controls over the State's IT systems. The worksheet is entitled "Application Specific Controls" and should be used to evaluate controls related to each application that the Department/Agency deems critical in regard to accomplishing their business objectives. **This worksheet must be completed for each application determined to be critical**. **NOTE** An example of a risk assessment tool (xls) (pdf) that can be used in assessing critical applications is provided along with the worksheets on the OFM website.

The worksheet is segregated into four (4) primary CobiT domains: Planning and Organization (PO), Acquisition and Implementation (AI), Delivery and Support (DS), and Monitoring (M). Within the four domains, there are 34 high-level IT processes identified. Each IT process has an associated CobiT control objective, which will need to be evaluated to determine if adequate controls are in place to meet that control objective. In addition to the worksheet, it may be necessary for the individuals completing the worksheet to refer to the detailed CobiT control objectives document. The control objectives document contains statements of the desired results or purposes to be achieved by implementing specific control procedures within an IT Process.

The worksheet is divided into sections. At the beginning of each section is a definition of the overall objective for that control and the potential/likely risks resulting by not having the control(s) in place.

At the end of each section is the **conclusion**. This is where the person filling out the form would summarize an overall conclusion of effective controls for each section. Any material weaknesses or reportable conditions present would be mentioned here as well as all other weaknesses.

At the end of each worksheet is the **certification**. This section is to be filled out and signed by the person with overall responsibility for the application. Note: If "Yes" is selected, then a list of material weaknesses must be attached.

The columns within the worksheet are described as follows:

- *Optimal Internal Controls (Column 1)* - Summarizes typical elements of a management and control structure that would address risks applicable to each IT process.

- *COBIT Reference (Column 2)* - This references the corresponding CobiT detailed control objective. (See the CobiT detailed control objectives document.)

- *Responsible Activity (Column 3)* - **Identify the activity and business owner responsible for each IT process** (e.g. Agency, Bureau, Division, or Office).

- *Columns 4 & 5* - **(Answer the questions from Column 1)** Enter check marks to denote whether appropriate controls exist within the IT application being evaluated; and whether controls are documented, effective, and sufficient.

Existence:
Documented
Not Documented
No Control in Place
Not Applicable

Performance/Effectiveness:
Excellent
Very Good
Satisfactory
Ineffective/Insufficient
Not Applicable

NOTE: If a control is under development or in process, performance should be categorized as Ineffective/Inefficient, not as Excellent, Very Good or Satisfactory.

- *Description/Comments (Column 6)* - Enter description/comments related to information and conclusions made in previous columns; identify formal policies, procedures, and informal practices that represent internal controls related to the IT Process. Identify, at a minimum, control objectives for which appropriate control activities do not currently exist, whether there are alternative or compensating controls, and whether plans and time frames exist for addressing deficiencies in the control structure. **This column must be completed.**

  NOTE: Attach a supplemental sheet if you are not able to fit all relevant information in this column

- *Monitoring (Column 7)* - Enter descriptions of activities performed to ensure that the controls in place are working (e.g. management reviews, comparisons, and/or reconciliations). Monitoring activities can be periodic or ongoing. Monitoring asks: How do you know the internal controls are working and what activity or process let's you know when they are not working? Examples of monitoring activities that inform you when things are working or not working effectively include: daily, weekly, monthly activities or processes such as log reviews, complaint follow-up telephone calls, and periodic evaluations or questionnaires. **This column must be completed.**

  NOTE: When possible, obtain applicable documentation and/or flowcharts for your future needs/requirements. If a control is not monitored, performance should be categorized as Ineffective/Inefficient, not as Excellent, Very Good or Satisfactory.

- *Attachments/Documentation* – Listed below are examples of types of documents that may be attached to explain what controls are in place that you have said were documented. This list is not all-inclusive.

  Contingency plans
  Test documentation
  User manuals
  Risk Assessments
  Service level agreements
  Position descriptions
  Meeting minutes
  Training materials
  Status reports
  Vendor hardware and software documentation
  Policy and procedure manuals
  Operations manuals
  Performance standards
  Output reports
  Organization charts
  Budgets
  Audit trails
  Source documents